

CYBER SECURITY GUIDELINES

Internet is just like life. It is interesting and we spend a lot of time doing amusing things here, but it comes with its fair share of trouble. With the technology boom and easy Internet access across the country, cyber crime, too, has become a pretty common occurrence. From hacking into computers to making fraudulent transactions online, there are many ways in which we can become a victim of illegal cyber activities.

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could also be misused for criminal activities. Today, there are many disturbing things happening in cyberspace. Cybercrime refers to all the activities done with criminal intent in cyberspace. These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium. Because of the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. The field of Cybercrime is just emerging and new forms of criminal activities in cyberspace are coming to the forefront with the passing of each new day.

To regulate such activities that violate the rights of an Internet user, the Indian government has the Information Technology Act, 2000, in place. Here are some of its sections that empower Internet users and attempt to safeguard the cyberspace.

In simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

NATIONAL CYBER SECURITY STRATEGY 2020 (NCSS 2020)

1. **Need for NCSS 2020** India was one of the first few countries to propound a futuristic National Cyber Security Policy 2013 (NCSP 2013). Since the adoption of NCSP 2013, the technologies, platforms, threats, services and aspirations have changed tremendously. The transformational Digital India push as well as Industry 4.0 is required to be supported by a robust cyberspace. However, Cyber intrusions and attacks have increased in scope and

sophistication targeting sensitive personal and business data, and critical information infrastructure, with impact on national economy and security. The present cyber threat landscape poses significant challenges due to rapid technological developments such as Cloud Computing, Artificial Intelligence, Internet of Things, 5G, etc. New challenges include data protection/privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, international cooperation on cybercrime & cyber terrorism, and so on. Threats from organised cybercriminal groups, technological cold wars, and increasing state sponsored cyber-attacks have also emerged. Further, existing structures may need to be revamped or revitalised. Thus, a need exists for the formulation of a National Cyber Security Strategy 2020.

2. **Formulation** The Indian Government under the aegis of National Security Council Secretariat through a well-represented Task Force is in the process of formulating the National Cyber Security Strategy 2020 (NCSS 2020) to cater for a time horizon of five years (2020-25).

3. **Vision Proposed** vision is to ensure a safe, secure, trusted, resilient and vibrant cyber space for our Nation's prosperity.

4. **Pillars of Strategy** We are examining various facets of cyber security under the following pillars: -

- a. Secure (The National Cyberspace)
- b. Strengthen (Structures, People, Processes, Capabilities)
- c. Synergise (Resources including Cooperation and Collaboration)

5. **Submissions** We wish to get your views on each of the above-mentioned aspects. You may comment, on any or all of the above-mentioned aspects or additional aspects, in a constructive and meaningful manner. Please contribute to make this strategic document a comprehensive 'whole-of-nation' approach for securing our cyberspace.

CYBER-CRIME - APPLICABILITY OF LEGAL SECTIONS

PENALTIES, COMPENSATION AND ADJUDICATION SECTIONS

Section 43 – Penalty and Compensation for damage to computer, computer system
If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network –

Accesses or secures access to such computer, computer system or computer network or computer resource shall be liable to pay damages by way of compensation to the person so affected.

Section 43A – Compensation for failure to protect data Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.

Section 44 – Penalty for failure to furnish information or return, etc. If any person who is required under this Act or any rules or regulations made there under to –

Furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

Section 45 – Residuary Penalty Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Section 65 – Tampering with Computer Source Documents If any person knowingly or intentionally conceals, destroys code or alters or causes another to conceal, he shall be punishable with imprisonment up to three years, or with fine up to two lakh rupees, or with both.

Section – 66 Computer Related Offences If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.

Section 66A – Punishment for sending offensive messages through communication service
Any person who sends, by means of a computer resource or a communication device,
Any information that is grossly offensive or has menacing character;

Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

Section 66B – Punishment for dishonestly receiving stolen computer resource or communication device. Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C – Punishment for identity theft Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D – Punishment for cheating by personation by using computer resource Whoever, by means of any communication device or computer resource cheats by personating; shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E – Punishment for violation of privacy Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, Explanation

Section-66F Cyber Terrorism with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by denying or cause the denial of access to any person authorized to access computer resource













Section 67 – Punishment for publishing or transmitting obscene material in electronic form Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or

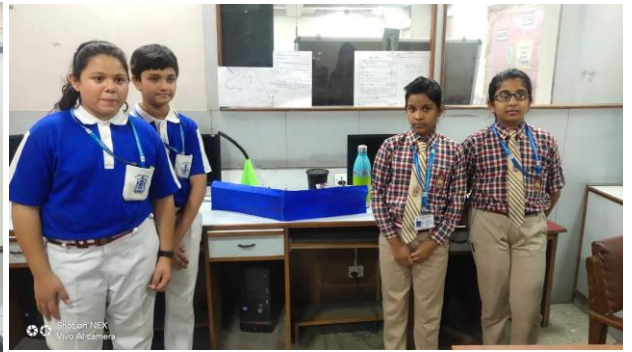
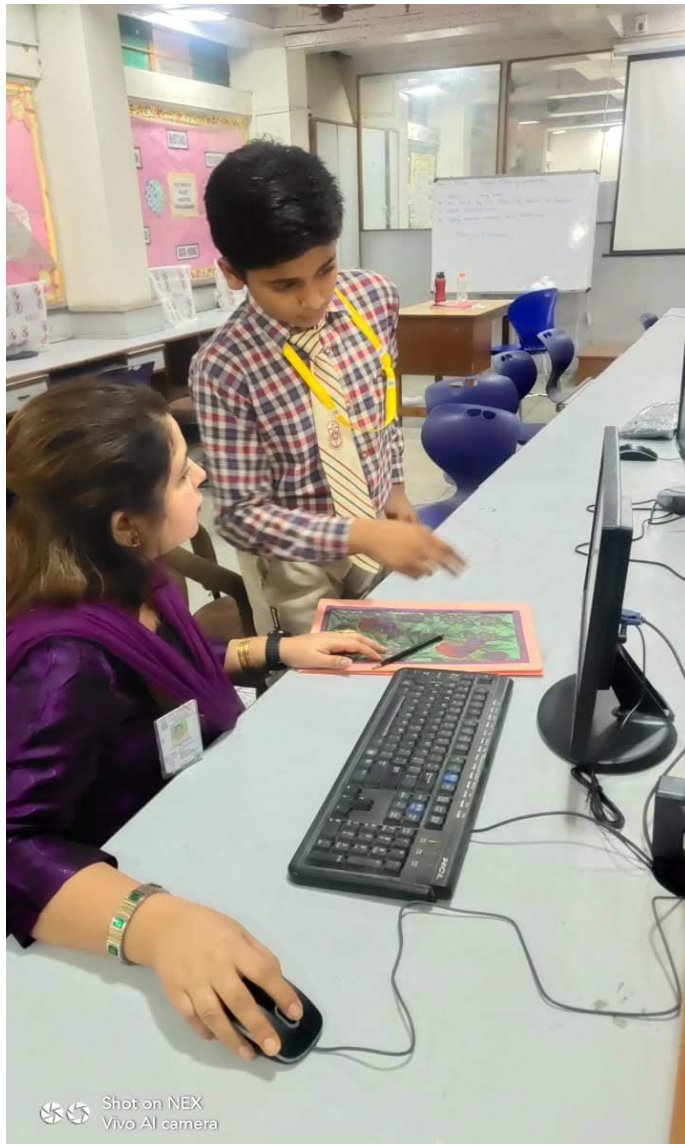
conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form publishes or transmits material in any electronic form which depicts children engaged in sexually explicit act or conduct shall be punished.

CYBER SAFETY CHECKLIST FOLLOWED AT N.K. BAGRODIA PUBLIC SCHOOL, ROHINI

-  School has a clear policy on cyber use and behavior
-  Students are not permitted to carry or use any electronic communication devices without prior permission.
-  Access to computer rooms is supervised by teachers.
-  Online educational activities are supervised and monitored.
-  There is internet security that restricts access to unsolicited contents.
-  Social networking sites are blocked at all times in the school.
-  Students are regularly educated in an age appropriate manner, on safe usage of technology and how to be responsible digital citizen.
-  Students are regularly educated in an age appropriate manner to understand the consequences under the laws –it act, jj act, ipc sections and pocso on cyber misuse, bullying, harassment/abuse on facebook, twitter, youtube etc.
-  School authority and children are oriented on procedures to be followed and steps prescribed within the legal framework in the event of cyber abuse or cyber crime incidents.
-  Experts are approached for facilitating the initial training and maintain record of date of training.
-  Parents and teachers and other staff members are sensitized on the school cyber policy and the safe usage of technology, internet usage in cyber cafes.
-  There is proper handling of e-waste by the school and students are trained for the same.

Cyber week is celebrated every year to make students aware about issues related with cyber security. Questions concerning Cyber ethics are asked in Computer quiz.



A workshop was conducted by Mr. Rakshit Tandon (Cyber Security Expert) for students and teachers who shared useful tips related with usage of mobile phone and internet.



A webinar was also attended by certain teachers related with cyber security by Dr. Pawan Duggal (Cyber law expert).

(West, Central, North & North West)
in association with

Action Committee
Unaided Recognised Private Schools (REGD.)

Action Talk **CYBER GUARDING & e-SCHOOLING**

Special Attendees

MS. NEETI SURI MISHRA
Judge/Secretary
Central DLSA

SHRI SANDEEP GUPTA
Judge/Secretary
North DLSA

SHRI VINOD MEENA
Judge/Secretary
West DLSA

Speaker
DR. PAWAN DUGGAL
Cyber Law Expert

Internet Guidelines For Students:

- ✓ The Internet is the global storehouse for information. It is like having the biggest library in the World at your fingertip Use the net to increase your knowledge, to do class work better.
- ✓ Visit interesting places sitting at your computer - visit the Taj or the Smithsonian Institution or the Louvre in Paris - all without stirring from your chair.
- ✓ Use the net to keep in touch with children from other parts of the Country or other Countries-make new pen friends; collect information. Many on-line service providers host chat rooms especially for children, monitored continuously for safety.
- ✓ The net is a global community - without any barriers, distances, boundaries.
- ✓ Be careful about talking to "strangers" on a computer network.
- ✓ Respect privacy on the net. You may have known the password of some other user- your friend/schoolmate. But do not use it to read their mail or send mail from their ID. Remember somebody else can also do this to you.
- ✓ Use the net to find information about schools and colleges-events or courses they may be offering. Many of them offer you a virtual guided tour of their facilities. Take advantage of this. This will help you take a decision when planning your future.
- ✓ Be careful about what you download from the net. Use a virus scan before the download as many programs may contain virus-this has the potential to destroy your system.

Don'ts :

- ✓ Do not give your password to anybody. Somebody who is malicious can cause great harm to you and your reputation. It is like leaving your house open for a stranger and walking away.
- ✓ When talking to somebody new on the net, do not give away personal information-like numbers of the credit card used by your parents, your home addresses/ phone numbers and such other personal information. If you feel uncomfortable or threatened when somebody on the net feeds you an improper or indecent message inform your parents or elders.
- ✓ Do not break into somebody else's computer and worse still change things; you are probably destroying a lifetime of hard work by somebody. You may be intelligent but use your intelligence for better things. Somebody else can be as ruthless and as intelligent to break into your

system and destroy your creations as well.

- ✓ Do not copy a program that is copyrighted on the net. It is illegal. You are actually stealing somebody else's hard work. There is a lot of illegally available material on the net. Do not use it yourself.

Hacking :

Hacking is an offence under section 66 of the IT Act. Hacking attracts serious penalties which include a jail term of 3 years, a fine of Rs. 2 Lakh or both.

National Cyber Crime Reporting Portal

This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.

Please contact local police in case of an emergency or for reporting crimes other than cyber crimes. National police helpline number is 100. National women helpline number is 181.

<https://www.cybercrime.gov.in/Webform/crmcondi.aspx>